UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/700,911	11/03/2003	Vipul Ved Prakash	6747P001	7777

7590 07/19/2007

John P. Ward
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
JACOBS, LASHONDA T	

ART UNIT	PAPER NUMBER
2157	

MAIL DATE	DELIVERY MODE
07/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/700,911	PRAKASH, VIPUL VED	
	Examiner	Art Unit	
	LaShonda T. Jacobs	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) *5,11 and 17* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-10, 12-16 and 18-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/29/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is responsive to Applicant's Amendment filed on June 29, 2007.

Claims 5, 11 and 7 have been cancelled. Claims 1, 7 and 13 have been amended. Applicant newly adds claims 19-24. Claims 1-4, 6-10, 12-16 and 18 are presented for further examination. Claims 19-24 are also presented for examination.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims **1-4**, **6-10**, **12-16** and **18-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (U.S. Pat. No.6,453,327) in view of Rounthwaite et al (hereinafter, "Rounthwaite", U.S. Pub. No. 2004/0177110) and in further view of McCormick et al (hereinafter, "McCormick", U.S. Pat. No. 6,421,709).

As per claim **1**, Nielsen discloses a method, comprising:

- receiving a plurality of reports from a community of users (col. 7, lines 62-67; Nielsen discloses receiving a junk mail reports from a members within a trusted group), each report identifying an email message as spam or not spam (col. 7, lines 47-63; Nielsen discloses a each member of the trusted group receiving a putative junk mail message and sending a junk mail report that classifies the message as junk e-mail); and

- determining if the email message is spam based on a number of the reports received from the community of users (col. 9, lines 20-35 and col. 13, lines 6-16; Nielsen discloses a trusted group server which maintains records of information relating to putative and junk mail. If the value of the number of trusted group reporting field exceeds a specified value the putative junk mail is considered to be junk mail).

Although, Nielsen discloses members of a trusted group sending junk mail reports to a trusted server. However, Nielsen does not explicitly disclose:

- a trust factor associated with each user.

Rounthwaite discloses a feedback loop for spam prevention system and method tat facilitate classifying items in connection with spam prevention in server and/or client based architectures comprising:

- a trust factor associated with each user (paragraph 0035, lines 1-9 and paragraph 0085; Rounthwaite discloses a trust level for each user to determine the user trustworthiness when classifying messages as spam or not).

Therefore, it would have been obvious to one of ordinary skill in the art at the time was made to modify Nielsen by incorporating or implementing a trust level for each trusted in member within the trusted group in order to determine the user trustworthiness for the purpose of classifying email message for spam prevention.

Nielsen in view of Rounthwaite discloses the invention substantially as claims discussed above.

However, Nielsen in view of Rounthwaite does not explicitly disclose:

- at least one signature based on a content of the email message.

McCormick discloses a system and method of filtering junk e-mails comprising:

- at least one signature based on a content of the email message (col. 11, lines 1-20; McCormick discloses generating a signature for the message based on the header and the body of the message).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nielsen in view of Rounthwaite by generating a signature for a message that is compared with other message signatures in order to determine whether or not the message is junk thus allowing unwanted email messages to be discarded.

As per claim **2**, Nielsen further discloses:

- maintaining a database of email messages determined as being spam (col. 9, lines 8-35; Nielsen discloses maintaining databases in the trusted user's client computer and in the trusted group's server relating to junk e-mail).

As per claim **3**, Nielsen further discloses:

- providing notifications to the community of users of email messages stored in the database and determined as being spam (col. 7, lines 50-67, col. 8, lines 1-3 and col. 13, lines 6-16; Nielsen discloses sending junk mail warning messages to the members in the trusted group regarding messages in the database that are considered to be junk mail).

As per claim **4**, Nielsen discloses:

- wherein each notification is in response to a request received from a user in the community for an indication on whether an identified message is spam (col. 7, lines 7, lines 50-67, col. 8, lines 1-3 and col. 13, lines 6-16; Nielsen discloses receiving junk

mail report from members within a trusted group in which the report indicates if a message is spam. After determining if the message is spam, the trusted group server sends a junk mail warning messages to the members in the trusted group regarding messages in the database that are considered to be junk mail).

As per claim **6**, Nielsen discloses the claimed invention substantially as claims discussed above.

However, Nielsen does not explicitly disclose:

- wherein the trust factor is based on an indication of how accurately previous reports sent by the user identified email messages as spam.

Rounthwaite discloses a feedback loop for spam prevention system and method tat facilitate classifying items in connection with spam prevention in server and/or client based architectures comprising:

- wherein the trust factor is based on an indication of how accurately previous reports sent by the user identified email messages as spam (paragraph 0035, lines 1-9 and paragraph 0085; Rounthwaite discloses a trust level for each user to determine the user trustworthiness when classifying messages as spam or not based on analyzing the number of contradictions, the number of changed minds, etc.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time was made to modify Nielsen by incorporating or implementing a trust level for each trusted in member within the trusted group in order to determine the user trustworthiness for the purpose of classifying email message for spam prevention.

As per claim **7**, Nielsen discloses a server, comprising:

- a processor (col. 7, lines 4-7); and
- a memory coupled to the processor, the memory storing instructions which when executed by the processor cause the processor to perform a method (col. 7, lines 4-17), comprising:
- receiving a plurality of reports from a community of users (col. 7, lines 62-67; Nielsen discloses receiving a junk mail reports from a members within a trusted group), each report identifying an email message as spam or not spam (col. 7, lines 47-63; Nielsen discloses a each member of the trusted group receiving a putative junk mail message and sending a junk mail report that classifies the message as junk e-mail); and
- determining if the email message is spam based on a number of the reports received from the community of users(col. 9, lines 20-35 and col. 13, lines 6-16; Nielsen discloses a trusted group server which maintains records of information relating to putative and junk mail. If the value of the number of trusted group reporting field exceeds a specified value the putative junk mail is considered to be junk mail).

Although, Nielsen discloses members of a trusted group sending junk mail reports to a trusted server. However, Nielsen does not explicitly disclose:

- a trust factor associated with each user.

Rounthwaite discloses a feedback loop for spam prevention system and method tat facilitate classifying items in connection with spam prevention in server and/or client based architectures comprising:

- a trust factor associated with each user (paragraph 0035, lines 1-9 and paragraph 0085; Rounthwaite discloses a trust level for each user to determine the user trustworthiness when classifying messages as spam or not).

Therefore, it would have been obvious to one of ordinary skill in the art at the time was made to modify Nielsen by incorporating or implementing a trust level for each trusted in member within the trusted group in order to determine the user trustworthiness for the purpose of classifying email message for spam prevention.

Nielsen in view of Rounthwaite discloses the invention substantially as claims discussed above.

However, Nielsen in view of Rounthwaite does not explicitly disclose:

- at least one signature based on a content of the email message.

McCormick discloses a system and method of filtering junk e-mails comprising:

- at least one signature based on a content of the email message (col. 11, lines 1-20; McCormick discloses generating a signature for the message based on the header and the body of the message).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nielsen in view of Rounthwaite by generating a signature for a message that is compared with other message signatures in order to determine whether or not the message is junk thus allowing unwanted email messages to be discarded.

As per claim **8**, Nielsen discloses:

- wherein the method further comprises maintaining a database of email messages determined as being spam (col. 9, lines 8-35; Nielsen discloses maintaining databases

in the trusted user's client computer and in the trusted group's server relating to junk e-mail).

As per claim **9**, Nielsen further discloses:

- providing notifications to the community of users of email messages stored in the database and determined as being spam (col. 7, lines 50-67, col. 8, lines 1-3 and col. 13, lines 6-16; Nielsen discloses sending junk mail warning messages to the members in the trusted group regarding messages in the database that are considered to be junk mail).

As per claim **10**, Nielsen discloses:

- wherein each notification is in response to a request received from a user in the community for an indication on whether an identified message is spam (col. 7, lines 7, lines 50-67, col. 8, lines 1-3 and col. 13, lines 6-16; Nielsen discloses receiving junk mail report from members within a trusted group in which the report indicates if a message is spam. After determining if the message is spam, the trusted group server sends a junk mail warning messages to the members in the trusted group regarding messages in the database that are considered to be junk mail).

As per claim **12**, Nielsen discloses the claimed invention substantially as claims discussed above.

However, Nielsen does not explicitly disclose:

- wherein the trust factor is based on an indication of how accurately previous reports sent by the user identified email messages as spam.

Rounthwaite discloses a feedback loop for spam prevention system and method tat facilitate classifying items in connection with spam prevention in server and/or client based architectures comprising:

- wherein the trust factor is based on an indication of how accurately previous reports sent by the user identified email messages as spam (paragraph 0035, lines 1-9 and paragraph 0085; Rounthwaite discloses a trust level for each user to determine the user trustworthiness when classifying messages as spam or not based on analyzing the number of contradictions, the number of changed minds, etc.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time was made to modify Nielsen by incorporating or implementing a trust level for each trusted in member within the trusted group in order to determine the user trustworthiness for the purpose of classifying email message for spam prevention.

As per claim **13**, Nielsen discloses a computer-readable medium having stored thereon a sequence of instructions which when executed by a computer, cause the computer to perform a method comprising:

- receiving a plurality of reports from a community of users (col. 7, lines 62-67; Nielsen discloses receiving a junk mail reports from a members within a trusted group), each report identifying an email message as spam or not spam (col. 7, lines 47-63; Nielsen discloses a each member of the trusted group receiving a putative junk mail message and sending a junk mail report that classifies the message as junk e-mail); and

- determining if the email message is spam based on a number of the reports received from the community of users(col. 9, lines 20-35 and col. 13, lines 6-16; Nielsen discloses a trusted group server which maintains records of information relating to putative and junk mail. If the value of the number of trusted group reporting field exceeds a specified value the putative junk mail is considered to be junk mail).

Although, Nielsen discloses members of a trusted group sending junk mail reports to a trusted server. However, Nielsen does not explicitly disclose:

- a trust factor associated with each user.

Rounthwaite discloses a feedback loop for spam prevention system and method tat facilitate classifying items in connection with spam prevention in server and/or client based architectures comprising:

- a trust factor associated with each user (paragraph 0035, lines 1-9 and paragraph 0085; Rounthwaite discloses a trust level for each user to determine the user trustworthiness when classifying messages as spam or not).

Therefore, it would have been obvious to one of ordinary skill in the art at the time was made to modify Nielsen by incorporating or implementing a trust level for each trusted in member within the trusted group in order to determine the user trustworthiness for the purpose of classifying email message for spam prevention.

Nielsen in view of Rounthwaite discloses the invention substantially as claims discussed above.

However, Nielsen in view of Rounthwaite does not explicitly disclose:

- at least one signature based on a content of the email message.

McCormick discloses a system and method of filtering junk e-mails comprising:

- at least one signature based on a content of the email message (col. 11, lines 1-20; McCormick discloses generating a signature for the message based on the header and the body of the message).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nielsen in view of Rounthwaite by generating a signature for a message that is compared with other message signatures in order to determine whether or not the message is junk thus allowing unwanted email messages to be discarded.

As per claim **14**, Nielsen further discloses:

- maintaining a database of email messages determined as being spam (col. 9, lines 8-35; Nielsen discloses maintaining databases in the trusted user's client computer and in the trusted group's server relating to junk e-mail).

As per claim **15**, Nielsen further discloses:

- providing notifications to the community of users of email messages stored in the database and determined as being spam (col. 7, lines 50-67, col. 8, lines 1-3 and col. 13, lines 6-16; Nielsen discloses sending junk mail warning messages to the members in the trusted group regarding messages in the database that are considered to be junk mail).

As per claim **16**, Nielsen discloses:

- wherein each notification is in response to a request received from a user in the community for an indication on whether an identified message is spam (col. 7, lines 7, lines 50-67, col. 8, lines 1-3 and col. 13, lines 6-16; Nielsen discloses receiving junk

mail report from members within a trusted group in which the report indicates if a message is spam. After determining if the message is spam, the trusted group server sends a junk mail warning messages to the members in the trusted group regarding messages in the database that are considered to be junk mail).

As per claim **18**, Nielsen discloses the claimed invention substantially as claims discussed above.

However, Nielsen does not explicitly disclose:

- wherein the trust factor is based on an indication of how accurately previous reports sent by the user identified email messages as spam.

Rounthwaite discloses a feedback loop for spam prevention system and method tat facilitate classifying items in connection with spam prevention in server and/or client based architectures comprising:

- wherein the trust factor is based on an indication of how accurately previous reports sent by the user identified email messages as spam (paragraph 0035, lines 1-9 and paragraph 0085; Rounthwaite discloses a trust level for each user to determine the user trustworthiness when classifying messages as spam or not based on analyzing the number of contradictions, the number of changed minds, etc.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time was made to modify Nielsen by incorporating or implementing a trust level for each trusted in member within the trusted group in order to determine the user trustworthiness for the purpose of classifying email message for spam prevention.

As per claims **19**, **21** and **23**, Nielsen in view of Rounthwaite discloses the invention substantially as claims discussed above.

However, Nielsen in view of Rounthwaite does not explicitly disclose:

- wherein at least one signature comprises a hash calculated based on the content of the email message.

McCormick discloses a system and method of filtering junk e-mails comprising:

- wherein at least one signature comprises a hash calculated based on the content of the email message (col. 11, lines 32-52; McCormick discloses the message signature is a type of hashing function).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nielsen in view of Rounthwaite by incorporating or implementing a message signature with a hashing function in order to calculate a matching function on messages to generate the likelihood that the messages are equal thus allowing unwanted email messages to be discarded.

As per claims **20**, **22** and **24**, Nielsen in view of Rounthwaite discloses the invention substantially as claims discussed above.

However, Nielsen in view of Rounthwaite does not explicitly disclose:

- using the at least one signature as a key to store the email message in the database if the message is determined to be spam.

McCormick discloses a system and method of filtering junk e-mails comprising:

- wherein at least one signature comprises a hash calculated based on the content of the email message (col. 11, lines 1-20; McCormick discloses generating a signature for the message based on the header and the body of the message).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nielsen in view of Rounthwaite by generating a signature for a message that is compared with other message signatures in order to determine whether or not the message is junk thus allowing unwanted email messages to be discarded.

Response to Arguments

3. Applicant's arguments with respect to claims **1-4**, **6-10**, **12-16** and **18-24** have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LaShonda T. Jacobs whose telephone number is 571-272-4004. The examiner can normally be reached on 8:30 A.M.-5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LaShonda T Jacobs
Examiner
Art Unit 2157

ltj
July 13, 2007